VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Testování vlastností kvazigrup

Quasigroup Property Testing

2010

Josef Gazur

Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 *Studijního a zkušebního řádu pro studium v bakalářských programech VŠB-TU Ostrava*.

V Ostravě 7. května 2010 .....

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 7. května 2010 .....

Rád bych na tomto místě poděkoval těm, kteří mi pomohli s různými problémy, na které jsem při tvorbě narazil. Zejména bych pak chtěl poděkovat mému vedoucímu bakalářské práce Doc. Mgr. Jiřímu Dvorskému, Ph.D. za všechny rady, návrhy které mi pomohly zrealizovat jak praktickou tak teoretickou část.

Abstrakt

Práce se zabývá vlastnostmi vygenerovaných tzv. *kvazigrup*, které se používají především v zabezpečení a šifrování dat. Je zde popsána teorie o základní struktuře - *latinském čtverci*, dále pak o zmiňovaných kvazigrupách. Zejména k čemu tyto struktury slouží, jaké typy těchto struktur existují, jaké má který typ vlastnosti a v další části - jak a jakým způsobem se tyto struktury tvoří. Další kapitola popisuje program *Gnuplot*, pomocí nějž se vlastnosti kvazigrup znázorňují graficky. V poslední části jsou popsány metody, zpracovávající data z hashovacích funkcí, založených na vygenerovaných kvazigrupách. Metodami jsou myšleny algoritmy, zpracovávající data ze souboru, které jsou pak statisticky popsány a uloženy do nových souborů a nakonec zpracovány programem Gnuplot pro výsledné grafické znázornění vlastností testovaných kvazigrup.

Klíčová slova: Latinský čtverec, Kvazigrupa, Gnuplot, WebTREC

Abstract

Work deals with properties called *quasigroup* generated, which are mainly used in security and data encryption. It describes the theory of basic structure of *Latin square*, then the above mentioned quasigroups. In particular, what these structures are used, what types of these structures exist, what is the type of properties in other parts - how and what in a way these structures forms. The next chapter describes the program *Gnuplot*, by which the properties of quasigroups presented graphically. The last section describes the methods, data processing of the hash function, based on the generated quasigroups. Methods are meant algorithms, which processing data of the files that are then statistically described and saved to new files and then processed by Gnuplot for the resulting graphical representation of the properties tested quasigroup.

Keywords: Latin square, Quasigroup, Gnuplot, WebTREC

Seznam použitých zkratek a symbolů

LS	–	Latinský čtverec
PDF	–	Probability density function
DVD	–	Digital Video Disc
VŠB-TUO	–	Vysoká škola báňská - Technická univerzita Ostrava
pdf	–	Portable Document Format
png	–	Portable Network Graphics
eps	–	Encapsulated Postscript
jpeg	–	The Joint Photographics Experts Group

Obsah

1 Úvod

Cílem této práce je rozebrat problematiku struktur zvaných *kvazigrupy*, dále zpracovat data vytvořené z hašovacích funkcí. Tyto hašovací funkce jsou založeny právě na vygenerovaných kvazigrupách. Pomocí izotopie jsou vygenerovány kvazigrupy. Z nich jsou pak vytvořeny hašovací funkce, přes které se přehašují slova ze slovníku WebTREC. Je potřeba tedy zpracovat data z hašovacích funkcích a k nim vytvořit grafy, které znázorňují určité vlastnosti každé kvazigrupy. Dále je potřeba vypočítat určité parametry ke každé kvazigrupě. Testované kvazigrupy jsou řádu 256 a bylo jich vygenerováno celkem osm tisíc. Úkolem je tedy zpracovat všechny výsledné hašovací tabulky a vytvořit pro každou dva typy grafů a ke každé spočítat statistické údaje(např. empírická pravidla, chí kvadrát testy).

V druhé kapitole je pojednáno o základní konstrukci tzv. *latinském čtverci*. Třetí kapitola se zabývá *kvazigrupami*, tedy jaké mají vlastnosti a jakými způsoby se dají generovat. V další kapitole se seznámíme s programem *Gnuplot*, který se využívá pro tvorbu grafů. Pátá kapitola popisuje implementaci programu pro zpracování a zobrazení všech výsledků. Závěrečná kapitola obsahuje vlastnosti některých testovaných kvazigrup.

2 Latinské čtverce

Pojem *latinský čtverec* byl zaveden Leonhardem Eulerem, což byl jeden z nejlepších matematiků 18. století. Nejstarší příklad latinského čtverce (vztah 1) je z 18. století a je uveden na malé bronzové pamětní desce, která se nachází v Anglii, v tehdejším hrabství Cornwall. Latinské čtverce se využívají při konstrukci samoopravných kódů a také jsou základem matematických hádanek(např. *Sudoku*). V této kapitole bylo čerpáno z[1].

$$\begin{array}{cccc} shall & we & all & die \\ we & shall & die & all \\ all & die & shall & we \\ die & all & we & shall \end{array} \tag{1}$$

Definice 2.1 *Latinský čtverec je čtvercová tabulka o velikosti $n \times n$ prvcích. Je vyplněna n různými prvky tak, že v každém řádku a v každém sloupci se nesmí vyskytovat stejný prvek víc než jednou. Tedy každý prvek se musí vyskytnout právě jedinkrát v každém řádku i v každém sloupci.*

Nechť $A\{a_1, a_2, ..., a_n\}$ je konečná abeceda prvků. L je latinský čtverec(matice) o řádu n, pak l_{ij} bude prvek matice L.

Příklad latinského čtverce je uveden ve vztahu 2.

$$\mathbf{L} = \begin{bmatrix} 3 & 0 & 1 & 2 \\ 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 1 & 2 & 3 & 0 \end{bmatrix} \tag{2}$$

Latinské čtverce (Dále jen LS) můžeme považovat za násobící tabulky kvazigrup. Pro popis LS pomocí ortogonálního pole se používá uspořádané trojice $(i, j, p)|$ kde i je řádek, j reprezentuje sloupec a p znamená prvek na pozici *i-tého* řádku a *j-tého* sloupce. Pro $i, j = 1, 2, ..., n$ a $p \in A$, kde A je abeceda s n prvky. Pak toto pole obsahuje n^2 trojic. Příkladem je zápis: $P = \{(1, 1, a), (1, 2, c), (1, 3, b), (2, 1, b), (2, 2, a), (2, 3, c), (3, 1, c), (3, 2, b), (3, 3, a)\}$ znázorňuje LS na níže uvedeném vztahu 3.

$$\mathbf{L} = \begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix} \tag{3}$$

Definice 2.2 *LS je* normalizovaný *(nebo ve* standardní formě*), pokud platí, že první řádek i první sloupec jsou stejně (abecedně) seřazeny od nejmenšího prvku po největší.*

Tedy první řádek a první sloupec jsou např. v uspořádání {1,2,3,4}, jiná uspořádání (např. {4,3,2,1}, či jiná) porušují výše uvedenou definici. Na vztahu 4 je uveden příklad normalizovaného LS.

$$\mathbf{L} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix} \tag{4}$$

Pokud provádíme operace nad LS (např. výměna řádků, sloupců), pak dokážeme pomocí těchto operací vytvořit z jednoho LS jiné, odlišné LS. Řád LS n znamená počet unikátních prvků z nichž se LS tvoří. Tedy ze vztahu 4 je $n = 4$ a unikátní prvky jsou $0, 1, 2, 3$. Pokud známe počet normalizovaných LS R_n pro řád n a chceme spočítat kolik se dá vygenerovat celkem LS řádu n, pak platí tato rovnice:

$$L_n = n!(n-1)!R_n$$

Počet všech LS je znám pro řád $n \leq 11$. Tabulka č.1 znázorňuje počet latinských čtverců v závislosti na řádu LS

n	L_n
1	1
2	2
3	12
4	576
5	161280
6	812851200
7	61479419904000
8	10877603245908295680
9	5524751496156892842531225600
10	9982437658213039871725064756920320000
11	776966836171770144107444346734230682311065600000

Tabulka 1: Celkový počet latinských čtverců při různém řádu LS

Z tabulky je vidět že počet variací LS při vzrůstajícím řádu roste nesmírně rychle. Pokud budeme tvořit např. LS nad abecedou A, která má řád $n = 26$, pak vytvoříme minimálně 10^{294} kvazigrup či latinských čtverců.

3 Kvazigrupy

Kvazigrupa je algebraická struktura s jednou binární operací, která je grupoidem a ve které je navíc možné dělit. Na rozdíl od grupy nemusí být operace komutativní ani asociativní a nemusí existovat neutrální prvek. Kvazigrupa s neutrálním prvkem se nazývá lupa. Kvazigrupy jsou hojně využívány v kryptografii. Zdrojem k této teorii posloužila hlavně disertační práce[1].

Definice 3.1 *Kvazigrupa je pár $(Q, \circ)$, kde Q je množina a $\circ$ je binární operace nad množinou Q. Řád kvazigrupy je definován jako n, pokud platí: $|Q| = n$. Pro každé $a, b \in Q$ existují jednoznačně určená $x, y \in Q$ tak, že platí: $a \circ x = b$ a $y \circ a = b$*

Kvazigrupa vychází z latinských čtverců. Násobící tabulka kvazigrupy řádu n odpovídá latinskému čtverci řádu n. Vztah 5 zobrazuje příklad násobící tabulky kvazigrupy řádu $n = 4$. Každý latinský čtverec má určitý počet možností, ovšem to záleží na jeho řádu. Tyto možnosti můžeme použít jako násobící tabulky. Pokud se podíváme na vztah 5, pak je to jen jedna z 576 možných variant [1].

$\circ$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	1	2	3	0
3	3	0	1	2

(5)

3.1 Typy kvazigrup a jejich vlastnosti

Definice 3.2 *Kvazigrupě $(Q, \circ)$ říkáme* lupa, *pokud pro každé $x \in Q$ existuje neutrální prvek e splňující: $x \circ e = x = e \circ x$*

Pokud je kvazigrupa komutativní, pak je násobící tabulka kvazigrupy symetrická. Jestliže je kvazigrupa lupa s neutrálním prvkem $e \in Q$, pak e-tý řádek a e-tý sloupec násobící tabulky jsou identické s popisným řádkem či sloupcem tabulky kvazigrupy. Většina kvazigrup nesplňuje asociativitu, některé však ano, ale jejich počet je minimální. Například kvazigrupa řádu $n = 4$ má 576 možných variant a jen 16 z nich je asociativních. Vztah 6 znázorňuje kvazigrupu, která je zároveň i lupou, je komutativní a asociativní.

$\circ$	0	1	2	3
0	2	3	0	1
1	3	0	1	2
2	0	1	2	3
3	1	2	3	0

(6)

Definice 3.3 *Grupoid $(Q, \circ)$ je nazván* levou *či* pravou *kvazigrupou, pokud splňuje podmínku $a \circ x = b$ a $y \circ a = b$, přičemž $x, y \in Q$ jsou jedinečné pro všechny $a, b \in Q$.*

[1] vycházíme z tabulky 1

Definice 3.4 *Kvazigrupě Q říkáme idempotentní, pokud platí pro prvek $x \in Q$, že $x \circ x = x$*

Vztah 7 znázorňuje kvazigrupu, která je idempotentní.

$\circ$	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

(7)

3.2 Generování kvazigrup

Pokud chceme aby šifrovací algoritmy, které jsou většinou založené na velkých kvazigrupách, pracovaly co nejrychleji, potřebujeme tyto kvazigrupy nějakým způsobem efektivně ukládat, aby se operace uvnitř kvazigrupy rychle vypočítávaly.

Pro uložení kvazigrup a následné počítání operací můžeme využít tabulky. Pokud je kvazigrupa řádu n, pak musíme uložit n^2 prvků. Tabulkový typ úložiště však pro velké kvazigrupy není vhodný, je spíš nepoužitelný. Existuje hodně možností jak tento problém uložení řešit. Dokonce jde ukládat kvazigrupy libovolného řádu blížícího se nekonečnu.

Kvazigrupy(či latinské čtverce) mohou být generovány náhodně(tedy jejich hodnoty). To však zabírá mnoho času a navíc tento proces musí splňovat podmínky, aby byly hodnoty vygenerovány správně. Základní podmínka je, že v každém řádku a sloupci se může prvek vyskytovat jen jednou.

V této části kapitoly uvedeme několik metod pro ukládání kvazigrup, z nichž některé jsou i použitelné pro generování velkých kvazigrup. U některých metod se však rapidně snižuje rychlost výpočtu se zvyšujícím se řádem kvazigrupy. Pro konstrukci(generování) si vysvětlíme tyto metody:

1. prodloužení (prolongation)
2. přímý součin (direct product)
3. kritická množina (critical sets)
4. jedineční představitelé (system of distinct representatives)
5. izotopie (isotopism)

3.2.1 Prodloužení

Pokud je definována *průseč* (transversal) v daném latinském čtverci řádu n, pak dokážeme pomocí *prolongace* z tohoto LS vygenerovat LS řádu $n+1$. Ovšem ne každý LS má průseč.

Definice 3.5 *Průseč latinského čtverce řádu n je množina n buněk, jedna v každém řádku, jedna v každém sloupci, takových že žádné dvě neobsahují stejný symbol.*

Na vztahu 8 je vyobrazen LS (L) s průsečí a LS (K) bez průseče.

$$\mathbf{L} = \begin{bmatrix} 0 & \mathbf{1} & 2 & 3 \\ 1 & 0 & 3 & \mathbf{2} \\ 2 & 3 & \mathbf{0} & 1 \\ \mathbf{3} & 2 & 1 & 0 \end{bmatrix} \quad K = \begin{bmatrix} 0 & \mathbf{1} & 2 & 3 \\ 1 & 2 & 3 & \mathbf{0} \\ \mathbf{2} & 3 & 0 & 1 \\ \mathbf{3} & 0 & 1 & 2 \end{bmatrix} \tag{8}$$

Pokud chceme vytvořit z LS L_1 řádu n latinský čtverec L_2 o řádu $n+1$, pak musíme postupovat následovně:

- Původní LS zvětšíme o jeden řádek a jeden sloupec
- Pro každou buňku z průseče vyjmeme hodnotu buňky a tuto hodnotu dosadíme do prázdné buňky nového sloupce v témže řádku, odkud jsme hodnotu vyjmuli. Tutéž hodnotu dosadíme do nového řádku na pozici sloupce, kde byla původní hodnota.
- Novou hodnotu dosadíme na místa odkud jsme vyjmuli původní hodnoty průseče a také ji dosadíme na zbylou prázdnou pozici, což je průsečík posledního řádku a sloupce.

Na vztahu 9 je vidět vlastnost průseče LS (L_1), kdy se transformuje L_2 z původního L_1.

$$\mathbf{L_1} = \begin{bmatrix} 0 & \mathbf{1} & 2 & 3 \\ 1 & 0 & 3 & \mathbf{2} \\ 2 & 3 & \mathbf{0} & 1 \\ \mathbf{3} & 2 & 1 & 0 \end{bmatrix} \quad \mathbf{L_2} = \begin{bmatrix} 0 & 4 & 2 & 3 & 1 \\ 1 & 0 & 3 & 4 & 2 \\ 2 & 3 & 4 & 1 & 0 \\ 4 & 2 & 1 & 0 & 3 \\ 3 & 1 & 0 & 2 & 4 \end{bmatrix} \tag{9}$$

V Latinském čtverci můžeme najít více různých průsečí. Lze tedy říct, že pokud najdeme p různých průsečí v latinském čtverci řádu n, pak dokážeme vygenerovat latinský čtverec řádu $n+p$ výše uvedeným způsobem. Ovšem prvký různých průsečí musí být vždy na jiné pozici. Na vztahu 10 je LS řádu 4 se dvěmi různými průsečemi, ze kterého vygenerujeme jiný LS řádu 6.

$$\mathbf{L_1} = \begin{bmatrix} \mathbf{0} & \mathbf{1} & 2 & 3 \\ 1 & 0 & \mathbf{3} & \mathbf{2} \\ 2 & 3 & \mathbf{0} & \mathbf{1} \\ \mathbf{3} & \mathbf{2} & 1 & 0 \end{bmatrix} \quad \mathbf{L_2} = \begin{bmatrix} \mathbf{5} & \mathbf{4} & 2 & 3 & \mathbf{1} & \mathbf{0} \\ 1 & 0 & \mathbf{5} & \mathbf{4} & \mathbf{2} & \mathbf{3} \\ 2 & 3 & \mathbf{4} & \mathbf{5} & \mathbf{0} & \mathbf{1} \\ \mathbf{4} & \mathbf{5} & 1 & 0 & \mathbf{3} & \mathbf{2} \\ \mathbf{3} & \mathbf{1} & \mathbf{0} & \mathbf{2} & \mathbf{4} & \mathbf{5} \\ \mathbf{0} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{5} & \mathbf{4} \end{bmatrix} \tag{10}$$

3.2.2 Přímý součin

Metoda *přímého produktu* dokáže ze dvou menších LS vygenerovat jeden větší LS. Tedy kombinací dvěma menšími LS se vytvoří jeden větší LS.

Definice 3.6 *Nechť jsou dány latinské čtverce L a K o řádech m a n. Pak můžeme vytvořit z těchto dvou LS jeden latinský čtverec (přímý produkt) $M = L \times K$ řádu mn, který je definován takto:*

$$\{((i_m, i_n), (j_m, j_n); (k_m, k_n) \quad | \quad (i_m, j_m, k_m) \in L \wedge (i_n, j_n, k_n) \in K\}$$

Na vztahu 11 je LS L řádu 3 a LS K řádu 2 a výsledný přímý produkt(vztah 12) LS $L \times K$ řádu 6

$$\mathbf{L} = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \quad \mathbf{K} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{11}$$

$$\mathbf{L} \times \mathbf{K} \begin{bmatrix} (1,0) & (0,0) & (2,0) & (1,1) & (0,1) & (2,1) \\ (2,0) & (1,0) & (0,0) & (2,1) & (1,1) & (0,1) \\ (0,0) & (2,0) & (1,0) & (0,1) & (2,1) & (1,1) \\ (1,1) & (0,1) & (2,1) & (1,0) & (0,0) & (2,0) \\ (2,1) & (1,1) & (0,1) & (2,0) & (1,0) & (0,0) \\ (0,1) & (2,1) & (1,1) & (0,0) & (2,0) & (1,0) \end{bmatrix} \tag{12}$$

Výše uvedený přímý produkt není pro naše potřeby vhodně reprezentován. My nechceme nějaké dvojice, proto přiřadíme každé dvojici jeden prvek z nové abecedy. Budeme mít například abecedu $A \in \{0, 1, ..., 5\}$. Každé dvojici přiřadíme jeden prvek z abecedy A, např. tímto způsobem $(0,0) \Rightarrow 0$, $(0,1) \Rightarrow 1$, $(1,0) \Rightarrow 2$, $(1,1) \Rightarrow 3$, $(2,0) \Rightarrow 4$, $(2,1) \Rightarrow 5$. Z tohoto přiřazení nám vznikne níže uvedený LS(13).

$$\mathbf{L} \times \mathbf{K_{tr}} \begin{bmatrix} 2 & 0 & 4 & 3 & 1 & 5 \\ 4 & 2 & 0 & 5 & 3 & 1 \\ 0 & 4 & 2 & 1 & 5 & 3 \\ 3 & 1 & 5 & 2 & 0 & 4 \\ 5 & 3 & 1 & 4 & 2 & 0 \\ 1 & 5 & 3 & 0 & 4 & 2 \end{bmatrix} \tag{13}$$

3.2.3 Kritické množiny

Pokud bychom chtěli sestavit LS nějak náhodně, pak si uděláme tabulku a začneme do ni postupně vkládat jeden prvek po druhém, tak aby platily základní pravidla LS. Můžeme si všimnout že čím více prvků máme vyplněných, tak tím se nám zmenšuje počet možnosti kam a které prvky vkládat. *Kritická sada* je podmnožina všech prvků latinského čtverce, ze které se dotvoří celý latinský čtverec. Máme tedy dáno či vyplněno pár hodnot a z nich se pak logicky doplní zbylé prvky. V této podkapitole čerpám i ze zdroje[2].

Definice 3.7 *Částečný latinský čtverec řádu n je latinský čtverec s uspořádanou trojicí i, j, k nad konečnou abecedou $A\{a_1, a_2, ..., a_n\}$ splňující následující podmínky:*

1. *jestliže (i, j, k), $(i', j, k) \in P$, pak $i = i'$,*

2. *jestliže* $(i, j, k),\ (i, j', k) \in P$, *pak* $j = j'$ *a zároveň*

3. *jestliže* $(i, j, k),\ (i, j, k') \in P$, *pak* $k = k'$,

Příklad částečného LS CL a z něj doplněný jedinečný LS L je uveden na vztahu 14

$$\mathbf{CL}\begin{bmatrix} 0 & 1 & . & . & . \\ 1 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 2 \\ . & . & . & 2 & 3 \end{bmatrix} \quad \mathbf{L}\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix} \tag{14}$$

Částečný LS je tedy tabulka $n \times n$ prvků, ve které nejsou všechny buňky vyplněny. Pokud je buňka vyplněna prvkem, pak se tento prvek může vyskytnout jen jednou v daném řádku a jednou v daném sloupci. Je dokázáno, že počet prvků kritické sady, ze které dotvoříme unikátní LS se vypočítá jako $scs = \lfloor n^2/4 \rfloor$. Minimální pokrytí kritické sady je nejmenší počet prvků, ze kterého doplníme unikátní LS. Tedy s částečného LS lze doplněním prvků dotvořit unikátní LS.

Neminimální pokrytí kritické sady je na vztahu 15, kde CL je částečný LS a L je kompletní jedinečný LS doplněný z CL.

$$\mathbf{CL}\begin{bmatrix} 0 & . & . & . \\ . & 1 & . & . \\ . & 0 & 2 & . \\ . & . & . & 2 \end{bmatrix} \quad \mathbf{L}\begin{bmatrix} 0 & 2 & 1 & 3 \\ 2 & 1 & 3 & 0 \\ 3 & 0 & 2 & 1 \\ 1 & 3 & 0 & 2 \end{bmatrix} \tag{15}$$

3.2.4 Jedineční představitelé

Mezi další možnosti, jak konstruovat latinské čtverce je zapisovat řádek po řádku do prázdného LS. Tato možnost je založena na systému jednoznačných představitelů.

Definice 3.8 *Máme definovaný celek* $P = \{P_1, P_2, ..., P_n\}$*, který se skládá ze sady podmnožin množiny* M*. Dále máme množinu* $X = \{x_1, x_2, ..., x_n\}$*, která představuje systém jednoznačných představitelů(SDR) pro jednotlivé podmnožiny z celku* P*. Platí zde, že pro* $i \neq j \Rightarrow x_i \neq x_j$ *pro všechna* $x_i \in A_i$*.*

Jestliže naplníme první řádek LS, tak při vyplňování druhého řádku musíme hodnoty přeuspořádat tak, aby se v žádném sloupci nevyskytovaly stejné hodnoty. Tento postup platí i při vyplňování dalších řádků.

$$\mathbf{L_2}\begin{bmatrix} 0 & 2 & 4 & 3 & 1 \\ 2 & 1 & 0 & 4 & 3 \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \end{bmatrix} \tag{16}$$

Na vztahu 16 je vidět kolik máme možností při vyplňování 3 řádku. $X_1 = \{1, 3, 4\}$, $X_2 = \{0, 3, 4\}, X_3 = \{1, 2, 3\}, X_4 = \{0, 1, 2\} a X_5 = \{0, 2, 4\}$. Ovšem musíme dát pozor při výběru hodnot. Pokud bychom vybrali jako první tři hodnoty $\{1, 0, 2, 3, 4\}$, pak bychom narazili na problém u 4 sloupce, kde nemůžeme dosadit ani jednu ze zbývajících hodnot(3,4). Proto musíme vždy zvolit správné uspořádání prvků(uk. 17).

$$\mathbf{L_3} \begin{bmatrix} 0 & 2 & 4 & 3 & 1 \\ 2 & 1 & 0 & 4 & 3 \\ 1 & 0 & 3 & 2 & 4 \\ . & . & . & . & . \\ . & . & . & . & . \end{bmatrix} \tag{17}$$

Věta 3.1 *Každý částečný latinský čtverec řádu n vyplněný r řádky, kde $r \leq n$ může být vždy doplněn, tak aby platilo pravidlo pro LS.*

3.2.5 Izotopie

U kvazigrup většího řádu již musíme zohlednit metody, které chceme použít, protože při generování nám data zaberou hodně místa a samotné generování - tedy použité metody musí být efektivní, aby zabíraly co nejméně času. Pomocí *izotopie* lze generovat a efektivně ukládat kvazigrupy větších řádů(např. $n \geq 2^{16}$).

Definice 3.9 *Jsou dány dvě kvazigrupy $(Q_1, \cdot)$ a $(Q_2, \circ)$ se stejným řádem n. Dále existují uspořádané trojice (α, β, γ) s prostým zobrazením z množiny Q_1 na množinu Q_2, kterým říkáme izotopie Q_1 nad Q_2 pokud platí pro všechna $x, y \in G$ následující:*

$$\alpha(x) \circ \beta(y) = \gamma(x \cdot y)$$

Platí také, že Q_2 je izotopem primární kvazigrupy Q_1. Je dokázáno, že množina všech izotopií kvazigrupy řádu n tvoří grupu řádu $(n!)^3$.

Můžeme si všimnout, že pokud přehodíme řádky či sloupce, nebo přejmenujeme hlavičky násobící tabulku kvazigrupy $(Q_1, \cdot)$ pak z ní dokážeme získat násobící tabulku kvazigrupy $(Q_2, \circ)$. Z výše uvedeného vztahu platí také pro všechna $x, y \in H$:

$$x \circ y = \gamma^{-1}(\alpha(x) \cdot \beta(y))$$

Existuje však několik neobvyklých kvazigrup, jejichž operace se dají specifikovat obyčejnými aritmetickými operacemi. Mezi tyto neobvyklé kvazigrupy můžeme zařadit *kvazigrupu modulárního odčítání* $(Q, \circ_{ms})$(quasigroup of modular subtraction). Operace $\circ_{ms}$ je definovaná jednoduchým výrazem:

$$x \circ_{ms} y = x + (n - y) \; mod \; n, n = |Q|$$

Tato vlastnost nám umožňuje efektivně ukládat velmi rozměrné kvazigrupy. Stačí nám jen ukládat informaci o permutacích α, β a γ spolu s kvazigrupou, která je použita pro

generování dalších kvazigrup. Příklad kvazigrupy modulárního odčítání $(Q, \circ)$(vztah 18) a k ní izotopické kvazigrupy $(Q, \cdot)$ můžeme vidět na vztahu 19 pro hodnoty $\alpha = [1, 2, 3, 0]$, β $[3, 2, 1, 0]$ a γ $[2, 0, 3, 1]$.

$\circ$	0	1	2	3
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

(18)

$\cdot$	0	1	2	3
0	0	2	1	3
1	1	3	2	0
2	2	0	3	1
3	3	1	0	2

(19)

Skupina těchto kvazigrup tvořící izotopii ke grupám(či abelovským grupám) je velmi podstatná pro výzkum a je využívána v mnoha jiných aplikacích. Mezi známou podmnožinu kvazigrup patří také *mediální* kvazigrupy(medial quasigroup) a *T* - kvazigrupy.

Definice 3.10 *Mediální kvazigrupa je kvazigrupa pro jejíž jakoukoliv čtveřici prvků $a, b, c, d \in Q$ platí vlastnost:*

$$(a \circ b) \circ (c \circ d) = (a \circ c) \circ (b \circ d)$$

Z toho plyne, že každá komutativní kvazigrupa je vždy mediální kvazigrupou. Opakem mediálních kvazigrup jsou *T* - kvazigrupy.

Definice 3.11 *T - kvazigrupa $(Q, \circ)$je definována nad abelovskou grupou $(Q, +)$ vztahem $x \circ y = \alpha(x) + \beta(y) + c$, kde c je konstanta z množiny Q, α a β jsou automorfizmem grupy $(Q, +)$.*

4 Program pro tvorbu grafů - Gnuplot

Gnuplot je přenosný, jednoduchý program pro tvorbu grafů. *Gnuplot* podporuje mnoho operačních systému. Mezi ně patří: Linux, OS/2, MS Windows, OSX, VMS a mnoho dalších. Jeho zdrojový kód je chráněn autorskými právy, ale jinak je *Gnuplot* volně dostupný ke stažení (např. http://www.gnuplot.info/). Původně byl určen pro vědecké účely, především ke zobrazovaní matematických funkcí a naměřených dat. Časem se jeho funkčnost rozrostla a tak ho začalo používat víc uživatelů. *Gnuplot* je pod aktivním vývojem už od roku 1986.

4.1 Možnosti programu

Gnuplot podporuje hodně typů grafů jak ve 2D, tak ve 3D souřadnicovém systému. Mezi podporované typy patří např. vykreslování pomocí úseček, bodů, sloupců, impulzů, kontur, vektorových polí. Ve 3D pak využijeme povrchové, prostorové sloupce a další různé typy. Grafy se vykreslují většinou pomocí uživatelem zadaných funkcí(s využitím knihovních funkcí), ale můžou se i vykreslovat pomocí načtených dat ze souboru. Jde nastavit různé podmínky pro čtení dat ze souboru. Můžeme využít cyklů k načítání velkého množství souborů. Vzhled grafu a popisy se dají upravit podle velké škály kritérií, čili uživatel si může opravdu nastavit vzhled podle svého přání.

S *Gnuplot* pracujeme ve dvou režimech. První je interaktivní(tedy příkazový řádek), kdy postupně zadáváme příkazy, které nám nastaví určité vlastnosti a pak příkazem **plot** s parametry vykreslíme požadovaný graf. Druhou možností je zavolání dávkového souboru, kdy máme připraven v podstatě skript, ve kterém jsou obsaženy příkazy, které opět nastaví požadované vlastnosti a vykreslí graf. Pro lepší přehlednost můžeme do skriptu **vnořovat** jiné skripty pomocí příkazu **load**. Pokud spustíme *Gnuplot* s parametry, pak se tyto parametry berou jak vstupní soubory či skripty a začnou se vykonávat jeden po druhém, tak jak byly v pořadí zapsány.

Výstupní graf se nám implicitně zobrazí na obrazovku, ovšem není problém nastavit výstup do souboru(formáty: eps, jpeg, png, pdf, postscript, LaTeX, aj.). Pokud chceme grafy přímo vytisknout, pak můžeme přesměrovat výstup přímo na tiskárnu či plotr.

Program je vybaven celkem rozsáhlou nápovědou, kterou můžeme spustit v interaktivním režimu pomocí příkazu **help** nebo **?**. Je v ní popsaný každé použití funkce, či příkazu pro nastavení vlastností. Nápověda je obsažena i v podadresáři *docs* pod názvem *gnuplot.pdf*, který je umístěn v adresáři samotného *Gnuplot*. Můžeme využít i předem vytvořených příkladů, které mají příponu *.dem* a nacházejí se v podadresáři *demo* složky *Gnuplot*.

4.2 Příklad použití

Než začneme s tvorbou skriptů či psaní příkazů do příkazového řádku, je třeba si uvědomit pár základních věcí, aby nenastaly problémy:

- *Gnuplot* je *case-sensitive*, tedy rozlišuje malá a velká písmena při psaní příkazů,

- pokud píšeme příkaz, který obsahuje víc parametrů, pak tyto parametry musíme napsat ve správném pořadí, jinak by příkaz nefungoval,
- některé příkazy můžou zabírat hodně místa(tedy můžou být napsány na několik řádků), takovýto řádek zakončujeme obráceným lomítkem \ a můžeme pokračovat s příkazem na dalším řádku,
- pokud chceme používat příkazy klasického příkazového řádku, pak jen zadáme na začátku příkazu vykřičník *!*,
- na jednom řádku můžeme napsat víc příkazů, musíme je však oddělit středníky **;**, výjimku však tvoří příkazy **load** a **call**, které musí byt vždy uvedeny jako poslední,
- pokud voláme příkazem **load** *soubor* uzavřený v uvozovkách, pak říkáme programu aby zpracoval skript a respektoval tzv. escape sekvence (*n* - přechod na nový řádek). Jesliže bude soubor uzavřen do apostrofů(*load 'soubor'*), pak ve zpracování souboru budou ignorovány escape sekvence,
- jestliže píšeme skripty, pak můžeme používat komentáře. Tedy pokud začíná řádek znakem #, pak se bere jako komentář.

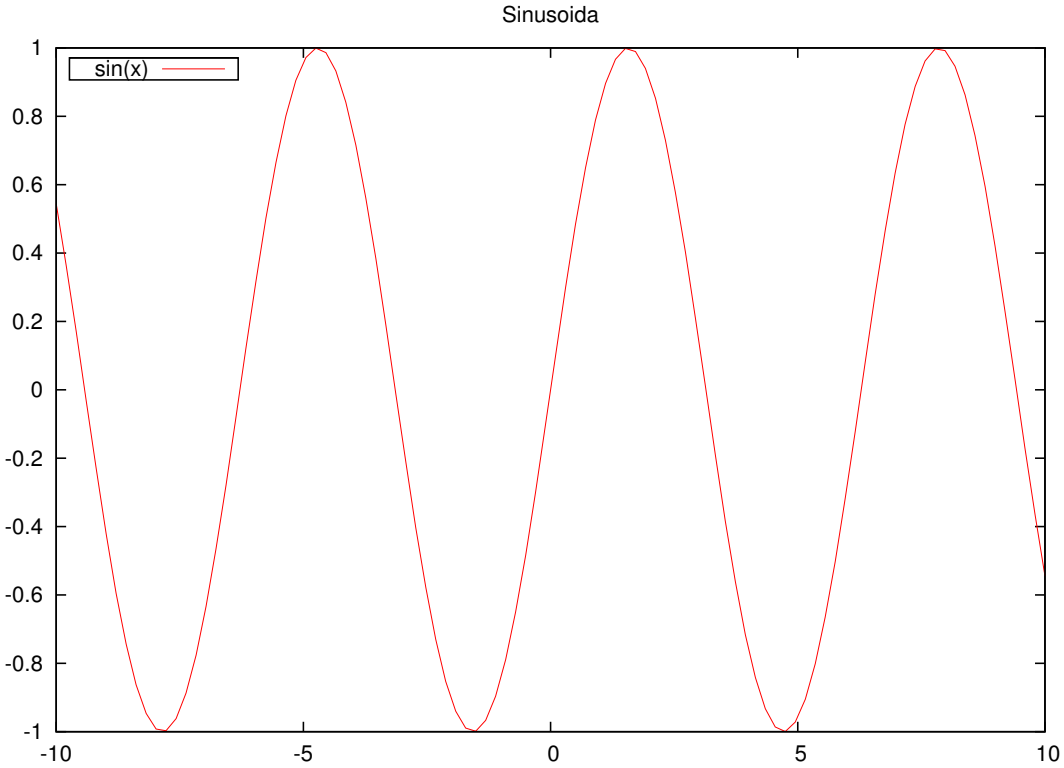
Jako první ukázku uvádím jednoduchý graf na obr. 1, vytvořený ze skriptu (výpis 1) *simple.dem*:

```
set terminal postscript eps color enhanced
set output 'simple.eps'
set key inside left top vertical Right noreverse enhanced autotitles box linetype -1 linewidth
    1.000
set samples 100, 100
set title "Sinusoida"
plot [-10:10] sin(x)
```

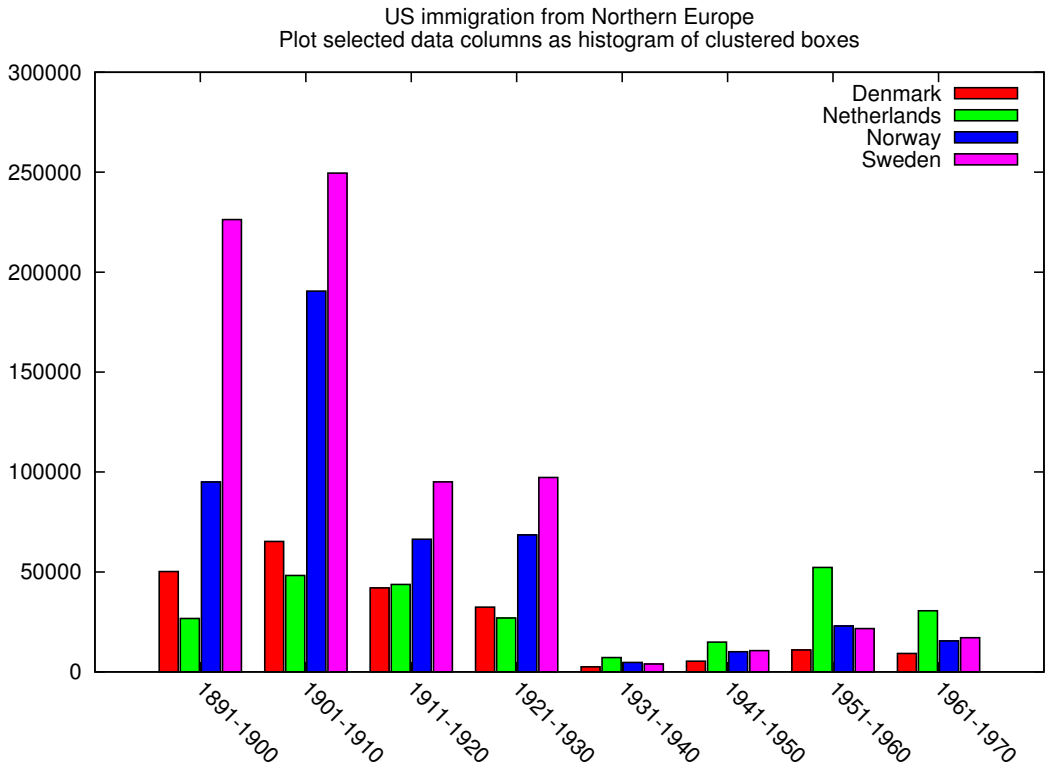
Výpis 1: Skript pro jednoduchý graf v Gnuplot

Zkusíme si popsat jednotlivé řádky skriptu:

1. řádek skriptu znamená nastavení kam bude směřován výstup, v našem případě do souboru s příponou **.eps**, další parametr - využití barevnosti,
2. řádek definuje název výstupního souboru,
3. řádek nastavuje popisek čáry grafu - kde má být umístěna(nahoře vlevo) a že bude ohraničena rámcem,
4. řádkem definujeme vzorkování(v našem případě je graf popsán 100 body, které jsou spojeny úsečkami),
5. řádek nastaví popisek(název) grafu,
6. příkazem říkáme, co má být vykresleno(z jakého intervalu a pomocí jaké funkce).



Obrázek 1: Graf funkce sinus



Obrázek 2: Histogram z datového souboru

Další příkladem bude skript (výpis 2), který vytvoří histogram ze souboru, kde jsou potřebná data. Ukázka grafu na obr. 2.

```
reset
set terminal postscript eps color enhanced
set output "emigration.eps"
set title "US␣immigration␣from␣Northern␣Europe\nPlot␣selected␣data␣columns␣as␣histogram␣of␣
    clustered␣boxes"
set auto x
set yrange [0:300000]
set style data histogram
set style histogram cluster gap 1
set style fill solid border -1
set boxwidth 0.9
set xtic rotate by -45
#set bmargin 10
plot 'immigration.dat' using 6:xtic(1) ti col, '' u 12 ti col, '' u 13 ti col, '' u 14 ti col
!epstopdf emigration.eps
```

Výpis 2: Skript pro histogram v Gnuplot

Nejdůležitějším příkazem je předposlední, kterým říkáme, že budeme data vykreslovat pomocí datového souboru. Přepínač **using** definuje, které sloupce se použijou jako

vstupní data. V tomto případě je *x-ová* hodnota načtena vždy z prvního sloupce a hodnoty y se berou z více sloupců(6, 12, 13 a 14), tím vznikají pro jednu hodnotu x čtyři hodnoty y.

Poslední příkaz převede výstupní soubor .eps na soubor .pdf, který je použitelnější pro načtení obrázku do dokumentu.

5 Implementace programu

Program má za úkol zpracovat vstupní data(prvky hašovací tabulky), jejichž výsledky (rozdělení) se budou znázorňovat pomocí grafů. Pro tyto účely bylo vygenerováno osm tisíc kvazigrup řádu 256. Tyto kvazigrupy byly vytvořeny pomocí *izotopie*. Z každé kvazigrupy je vytvořena *hašovací funkce*, přes kterou se „přehašujou" data ze slovníku *WebTREC*(viz. dále). Z toho nám vznikne „hašovací tabulka" s 256 řádky, přičemž na každém řádku je určitý počet stejných hašů(nabývají hodnot $0 - 255$). Z této tabulky se každá hodnota haše uloží do souboru, který je následně setříděn. Každý soubor tedy obsahuje na každém řádku jedno číslo z rozsahu 0 až 255. Celkem je v souboru 4319200 hašů.

WebTREC jsou slova extrahovaná z anglického textu. Slova byla extrahována z kolekce webových stránek WebTREC. Původní velikost textu byla cca 18 gigabajtů. Z tohoto textu byl sestaven slovník, který obsahuje celkem 4319200 unikátních slov. Tento soubor má simulovat hašování klíčů, tvořených textovými řetězci, do hašovacích tabulek.

Cílem experimentů[4] je ověřit rozložení pravděpodobnosti výskytu jednotlivých hodnot hašovací funkce pro danou kvazigrupu. Jako vstupní data v tomto případě sloužil soubor WebTREC.

Experiment probíhal následujícím způsobem:

1. Inicializace kvazigrupy Q řádu $256(2^8)$
2. Vytvoření hašovací tabulky o 256 slotech, kolize byly řešeny separátním řetězením.[2]
3. Pro každé slovo w ze vstupu byla vypočtena hodnota hašovací funkce $h_Q(w)$.
4. Slovo w bylo vloženo do hašovací tabulky do slotu s indexem $h_Q(w)$.

Je potřeba zpracovat všechny soubory a pro každý z nich vytvořit dva grafy. První graf bude histogram. Bude zobrazovat počet výskytů každého čísla(hašovací hodnoty) v souboru. Druhý graf bude opět histogram a bude znázorňovat počet výskytů *délky slotu* (z počtu výskytů každého čísla). Jednoduše řečeno, druhý graf bude histogramem prvního grafu(histogramu). V druhém grafu je potřeba znázornit i teoretické rozložení dat pomocí funkce *hustoty pravděpodobnosti normálního rozdělení*, k tomu je potřeba vypočíst ze vstupních dat několik potřebných statistických údajů(např. aritmetický průměr, rozptyl, empírické pravidlo, test dobré shody a další). Celkem je tedy potřeba vygenerovat šestnáct tisíc grafů.

Implementace programu je realizovaná v programovacím jazyku *Java*. Program je vytvořen tak, aby zpracoval vstupní data a výstupem jsou pak soubory pro realizaci histogramů v programu *Gnuplot*. Následně jsou vytvořeny jednoduché skripty pro zpracování všech souborů v programu *Gnuplot*. Programování je realizováno ve vývojovém prostředí *Netbeans*, které slouží pro ulehčení psaní kódů, podporuje automatické doplňování zdrojového kódů a další užitečné výhody.

[2] Zde se však nepoužívá tabulka. Používá se pole a hodnota na indexu klíče se vždy inkrementuje pokud hašovací klíč má stejnou hodnotu jako index pole.

5.1 Potřebné údaje

Pro tvorbu grafu četnosti délky slotů potřebujeme spočítat pár nezbytných statistických údajů[3]. Rozdělení grafu by mělo odpovídat *normálnímu(Gaussovému)* rozdělení. Ovšem se znázorněným histogramem potřebujeme znázornit i teoretické rozložení. Dále je potřeba vypočíst empirické pravidlo a test dobré shody(chí kvadrát test). Proto musíme vypočíst pár základních údajů. Mezi ně patří **aritmetický průměr**. Ten se vypočte následujícím vztahem:

$$\overline{x} = \frac{1}{m}\sum_{i=1}^{m}(x_i)$$

Kde m je celkový počet čísel a x_i pak číslo na *i–té* pozici. Pro náš účel se však hodí jiný vzorec:

$$\overline{x} = \frac{1}{m}\sum_{i=1}^{k}(n_i x_i)$$

Zde je tedy m opět celkový počet čísel, k je počet unikátních čísel, n je pak počet výskytů pro číslo x na *i–té*pozici.

Mezi další parametr patří **směrodatná odchylka**. Ta vypovídá o různosti prvků. Pokud je hodnota směrodatné odchylky velká, pak jsou prvky od sebe velmi odlišné. Jestliže je malá, potom se prvky od sebe moc neliší. **Směrodatná odchylka** σ se vypočítá následujícím vzorcem:

$$\sigma = \sqrt{\frac{1}{m}\sum_{i=1}^{k} n_i(x_i - \mu)^2}$$

Tento vztah je odvozen od obecného a pro naše účely se lépe hodí. Zde je m celkový počet čísel, k počet unikátních čísel, n je počet výskytů čísla x na *i–té* pozici a μ znamená aritmetický průměr.

Dalším parametrem je **rozptyl** σ^2. Ten se vypočítá jako obsah čtverce nad velikostí *směrodatné odchylky*.

$$\sigma^2 = \frac{1}{m}\sum_{i=1}^{k} n_i(x_i - \mu)^2$$

Rozptyl nebo též **variance** charakterizuje variabilitu pravděpodobného rozdělení náhodné veličiny v souboru dat.

Ze *směrodatné odchylky* dokážeme vypočíst **empirické pravidlo**. Empirické pravidlo se hodí ke zjištění pravděpodobnostního obsazení náhodné veličiny kolem střední hodnoty (aritm. průměru). Podle tabulky 2 by měly obsazení normální rozdělení vycházet následovně:

rozsah	populace v %
$\mu \pm \sigma$	cca 68%
$\mu \pm 2\sigma$	cca 95%
$\mu \pm 3\sigma$	cca 99%

Tabulka 2: Teoreticé rozložení populace

Pro každý soubor potřebujeme také zjistit **test dobré shody** (χ^2 test). Ten ověří zda se skutečně zjištěné hodnoty neodchylují příliš od očekávaných hodnot při určité hladině významnosti. Je potřeba vypočítat X^2 následujícím způsobem:

$$X^2 = \sum_{j=1}^{m} \frac{(X_j - np_j^0)^2}{np_j^0}$$

Kde m je počet odlišných(unikátních) jevů. X_j znamená četnost jevu A_j na *j–té* pozici, np_j^0 označuje teoretickou hodnotu(očekávanou četnost) vycházející z nějakého pravděpodobnostního modelu. My vycházíme z pravděpodobnostního modelu *hustoty pravděpodobnosti normálního rozdělení*(níže bude rozebráno). Podle tabulky *kritické hodnoty rozdělení* porovnáme náš výsledek X^2 s tabulkovým $\chi^2_{m-2-1}(\alpha)$, kde α znamená *hladinu významnosti*, kterou si zvolíme. Jestliže $X^2 \geq \chi^2_{m-2-1}$, pak zamítáme *nulovou hypotézu* na hladině významnosti α. Nulová hypotéza znamená očekávané rozdělení p_j^0 daného jevu A_j.

Víme, že by data měla odpovídat *normálnímu rozdělení* a my potřebujeme proložit tato data křivkou teoretického rozdělení. Pokud známe *aritmetický průměr* a *rozptyl*, můžeme křivku vytvořit pomocí funkce **hustoty pravděpodobnosti normálního rozdělení** (**PDF**). Ta je dána vztahem:

$$PDF = \frac{1}{\sqrt{2\pi\sigma^2}} \exp^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Přičemž μ je *aritmetický průměr* pro celý soubor čísel, σ pak *rozptyl* pro daný soubor a x je hodnota délky slotu(četnost čísla). Tuto funkci využijeme při počítání výše zmíněného χ^2 testu a také pro generování grafů ze skriptu.

5.2 Načítání dat ze souboru

Vstupní data jsou uloženy v *textových* souborech a aby zabraly co nejméně místa, jsou zabaleny(formát **.gz**). Je potřeba načíst přímo zabalené soubory, které se přečtou řádek po řádku a budou se ukládat do operační paměti do nějaké struktury (v našem případě do pole). V knihovnách *Javy* existují funkce kterým dáme na vstup cestu k souboru a ty nám umožní s tímto souborem manipulovat.

Na níže uvedeném výpisu 3 zdrojového kódu je příklad práce se (zabaleným) souborem.

```
public void vytvorCetnostCisel(File fileIn , File fileOut ) throws IOException {
    BufferedReader bReader;
```

```
    if ( fileIn .getName().endsWith("gz")) {
        InputStream gStream = new GZIPInputStream(new FileInputStream(fileIn));
        Reader decoder = new InputStreamReader(gStream, "UTF-8");
        bReader = new BufferedReader(decoder);
    }
    else {
        bReader = new BufferedReader(new FileReader(fileIn));
    }
    String radek;
    int readNumber;
    cetnostCisel = new int[cetnostCisel.length];
    pocetCisel = pocetSlotu = 0;
    while((radek = bReader.readLine()) != null) {
        readNumber = Integer.parseInt(radek);
        cetnostCisel[readNumber]++;
        pocetCisel++;
    }
    bReader.close();
    .
    .
    .
}
```

Výpis 3: Čtení a zpracování (zabaleného) vstupního souboru

Při první větvení programu se rozhoduje zda pracujeme se zabaleným textovým souborem či nikoliv. Pokud pracujeme, pak musíme použít specifický dekodér, který je pak předán čítači(využívající vyrovnávající paměť) jako parametr. V iterační smyčce pak čteme řádek po řádku, přičemž každý řetězec(číslo) v řádku převádíme na číselnou proměnnou a pro její index se zvýší hodnota o jednu.

5.3 Zápis dat do souboru

Pokud máme potřebná data načtená v poli, pak bude potřeba vytvořit soubor a do něj zapsat na každý řádek číslo a jeho četnost(počet výskytů). V našem případě je zápis realizován stylem: **číslo** *tabelátor* **četnost čísla** *přechod na nový řádek*.

Pro ukázku uvádím výpis 4 ze zdroj. souboru:

```
public void vytvorCetnostCisel(File fileIn , File fileOut ) throws IOException {
    .
    .
    .

    FileWriter fWriter = new FileWriter(fileOut);
    fWriter.write("#####################␣Data␣pro␣vytvoreni␣grafu␣cetnosti␣cisel␣
        ####################\n\n\n\n");
    for (int i = 0; i < cetnostCisel.length; i++) {
        if (cetnostCisel[i] > 0) {
            pocetSlotu++;
            fWriter.write(i + "\t" + cetnostCisel[i] + "\n");
        }
    }
```

```
        fWriter.close();
    }
```

Výpis 4: Zápis dat do souboru

Opět budeme pracovat s textovým souborem. Vytvoříme instanci knihovní třídy *Filewriter*, umožňující zápis dat do text. souboru. Použijeme cyklus *for* pro procházení celého pole a každý index a k němu přiřazenou hodnotu (pokud je hodnota nulová pak informaci ignorujeme) zapíšeme do souboru. Mezi indexem a jeho hodnotou uděláme mezeru a poté odřádkujeme.

Vytvoření všech potřebných souborů pro generování grafů zabralo cca dvě a půl hodiny na přenosném počítači s procesorem 1.8Ghz a pamětí 1.5GB.

5.4 Generování grafů

Kód napsaný v Javě vytvoří sadu souborů, ze kterých se budou generovat grafy. První sada budou soubory, obsahující data pro vytvoření grafů četnosti čísel. Na každém řádku bude *číslo, mezera(tabelátor), četnost čísla*. Druhá sada souborů budou potřebná data pro vytvoření histogramu četnosti délky slotů. Ty budou ve stejné struktuře jako první sada, akorát na prvních řádcích budou zakomentovány potřebné statistické údaje. Pro názornost uvedeme příklad části souboru (výpis 5).

```
##################### Data pro vytvoreni grafu cetnosti delky slotu ####################
#  Mean     = 16871.87109375
#  Median   = 16876.0
#  Mode     = 16797.0
#  Std      = 133.3079142436787
#  Variance = 17770.999999999996
#
#  Rule68   = 70.703125
#  Rule95   = 93.359375
#  Rule99.7 = 100.0
#
#  Chi kvadrat test  = pokud X^2 > nebo rovno chi^2 => zamitame nulovou hypotezu na hladine
     alfa
#  X^2 = 178.81016322126422 chi^2_210(q0.95) = 243.81493752766667
#  X^2 = 178.81016322126422 chi^2_210(q0.99) = 257.7507905693717


16518 1
16519 1
16553 1
16556 1
16557 1
16563 1
```

Výpis 5: Výpis z dat. souboru

Třetí sada obsahuje pouze dva řádky. Na prvním je uveden parametr aritmetický průměr a na druhém řádku je parametr rozptylu. Tato sada je potřebná pro vygenerování grafů s četnostmi délky slotů, které jsou proložený funkcí pro teoretické rozložení.

Pokud chceme spustit generování grafů stačí spustit dva skripty. První vygeneruje grafy pro četnost čísel, druhý pro četnost délky slotu. Pro představu uvedeme kód skriptu (výpis 6).

```
reset
set terminal postscript eps color enhanced
set title "Histogram cetnosti delky slotu. Typ rozlozeni: Gausovske, rozsah cisel: 0 - 255"
set xlabel "Delka slotu"
set ylabel "Cetnost delky slotu"
# inicializace citace pro iteraci
i = -1
# un ... pocet cisel z abecedy
un = 256
filein (n) = sprintf ("%dCDS.dat",n)
# !!! pozor, slozka grafyCDS musi byt vytvorena
fileout (n) = sprintf ("..\\grafyCDS\\%dCDS.eps",n)
filepar (n) = sprintf ("%dpar.gp",n)
# parametry mean a var jsou volany pri kazde iteraci zvlast ze souboru
pdf(x) = un*(1/sqrt(2*pi*var)) * exp(-((x - mean)**2)/(2*var)) + 1
load 'for.gp'
```

Výpis 6: Skript pro tvorbu grafů

Zde je vidět práci se soubory jako s parametry. Funkce *filein(n)*, *fileout(n)*,*filepar(n)* vrací řetězec(název souboru), se kterým se bude pracovat. Volají se v souboru *for.gp* a jako parametr se ji dává hodnota čítače. Pro ukázku uvedeme zdroj. kód tohoto souboru (výpis 7)

```
i = i + 1
set output fileout (i)
load filepar (i)
plot filein (i) with lines title "Experimentalni data", pdf(x) title "Teoreticke rozlozeni"
if (i < 7999) reread
```

Výpis 7: Skript pro definici smyčky

Jednoduchá definice iterační smyčky. Čítač inkrementujeme, nastavíme výstupní soubor pomocí funkce *fileout(i)*, kde parametrem bude hodnota čítače. Dále zavoláme soubor s potřebnými parametry a následně můžeme vykreslovat(v našem případě do souboru). Vše ukončíme podmínkou iterace. Pokud se je podmínka splněna zavoláme soubor se smyčkou znovu. Předpokladem správného chodu je správné pojmenování vstupních souborů, jejichž názvy jsou odlišeny pouze čísly.

6 Závěr

6.1 Ideální výsledky

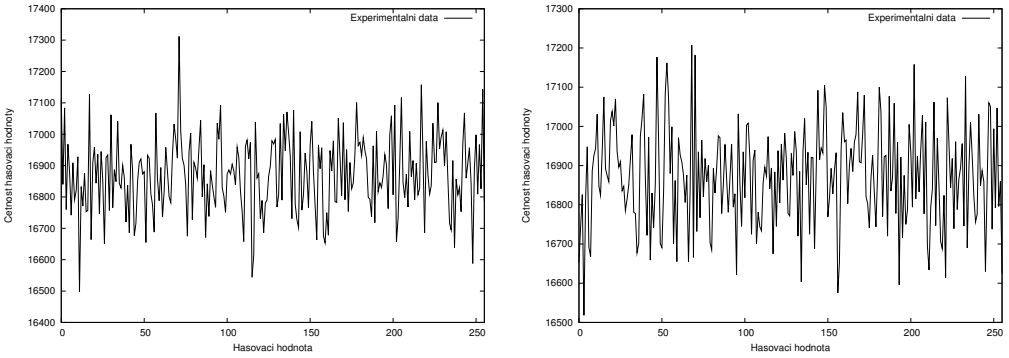
Ideálním výsledkem[4] v tomto experimentu je rovnoměrné rozdělení slov na vstupu po celé hašovací tabulce. Střední hodnota počtu slov v jednom slotu by měla odpovídat celkovému počtu slov na vstupu dělenému počtem slotů. Histogram délek slotů by v tomto případě měl kopírovat normální rozdělení.

6.2 Ukázky experimentálních výsledků

Ukážeme si rozdělení slov na dvou odlišných hašovacích funkcí. Jak je vidět z grafů3, tak každý zpracovaný soubor má trochu jiné rozdělení hašovacích hodnot. Toto rozdělení by se mělo podobat *uniformnímu* rozdělení. Na obr. 3(a) je vidět rozdělení hašovacích hodnot z hašovací funkce první kvazigrupy, na obr. 3(b) pak rozdělení z hašovací funkce páté kvazigrupy.

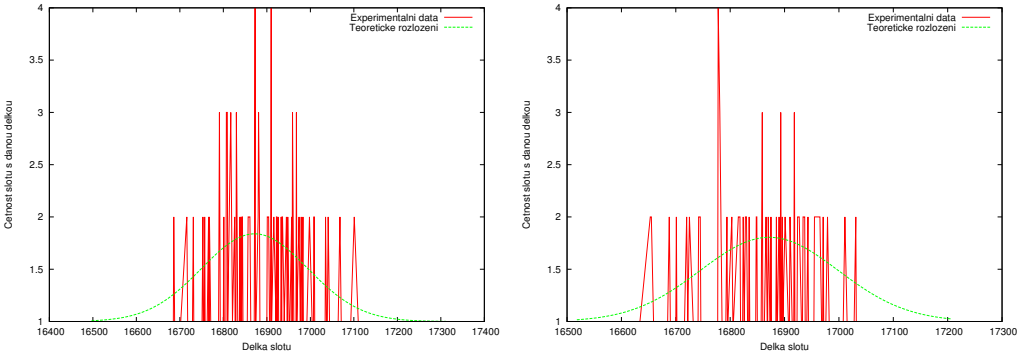
Pokud se podíváme na rozdělení délky slotů, tak opět každá kvazigrupa má odlišný průběh. Na grafu 4(a) je histogram rozdělení délky slotů první kvazigrupy, na 4(b) je rozdělení páté kvazigrupy. Ideální rozdělení je zobrazeno zelenou čarou.

Co se týče parametrů vypočítaných ke každé z kvazigrup, pak každá z nich je má také odlišné. Největší rozdíl je však poznat při výpočtu χ^2 testu, kdy některé kvazigrupy tento test nesplňují. Parametry, empirické pravidla a χ^2 testy jsou uvedeny v přílohách.



(a) kvazigrupa 1 řádu 255 (b) kvazigrupa 5 řádu 255

Obrázek 3: Rozdělení hašovacích hodnot z hašovacích funkcí dvou kvazigrup



(a) kvazigrupa 1 řádu 255 (b) kvazigrupa 5 řádu 255

Obrázek 4: Rozdělení délky slotů dvou kvazigrup

7 Literatura

[1] Eliška Ochodková, Non–associative Structures in Cryptography, Ostrava 2009

[2] J.A. Bate, G.H.J. van Rees, The Size of the Smallest Strong Critical Set in a Latin Square

[3] Karel Zvára a Josef Štěpán, Pravděpodobnost a matematická statistika

[4] Jiří Dvorský, Experimenty s kvazigrupami

A Obsah DVD

Na DVD jsou obsaženy všechna potřebná data pro testování a vyhodnocování.

A.1 Vstupní data pro testy

Vstupní data jsou zabalena ve složce *Slots*. Tato složka obsahuje celkem 8000 zabalených souborů. Po rozbalení mají všechny soubory velikost 160GB.

A.2 Výstupní data pro generování grafů

Výstupní data jsou opět zabalena v souboru *Data.zip* a jsou rozděleny do 4 složek. Ve složce *CC* jsou uloženy vstupní data pro tvorbu grafů délky slotů a dva skripty pro vytvoření těchto grafů. Spuštěním skriptu *histCC.dem* se všechny grafy vygenerují. Podmínkou je mít nahrán program *Gnuplot*. Ve složce *grafyCC* jsou obsaženy všechny výstupní grafy pro délku slotů. Další složka *CDS* obsahuje vstupní data pro tvorbu grafů četnosti délky slotů a opět dva skripty pro generování grafů. Spuštěním skriptu *histCDS.dem* se začnou generovat grafy pro četnost délky slotů. Poslední složka *grafyCDS* obsahuje všechny vygenerované grafy četnosti délky slotů.

A.3 Text bakalářské práce

Ve složce *BCThesis* najdeme elektronickou podobu této bakalářské práce ve formátu *pdf*.

A.4 Software

Složka *Kvazigrupy* obsahuje zdrojové kódy pro generování kvazigrup a zpracování dat. Složka *Bakalarka* obsahuje zdrojové kódy pro zpracování zabalených vstupních souborů(hašovacích tabulek) bakalářské práce.

B Permutace užité pro vytváření testovacích izotopických kvazigrup

V tabulce 3 jsou uvedeny permutace užité pro vytváření izotopických kvazigrup. Permutace jsou označeny identifikačním číslem (Id) v rozsahu 0 až 19. Dále, máme-li permutaci

$$\pi = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

je v tabulce z důvodu úspory místa zapsána jen posloupnost $b_1\ b_2\ \dots\ b_n$. Posloupnost $a_1\ a_2\ \dots\ a_n$ má stále stejný tvar 0 1 2 ... 254 255.

Tabulka 3: Permutace užité pro vytváření testovacích izotopických kvazigrup

Id	Permutace
0	(25, 172, 134, 214, 114, 5, 179, 148, 105, 9, 10, 173, 12, 200, 195, 243, 72, 69, 82, 35, 183, 40, 233, 211, 166, 160, 26, 27, 80, 182, 93, 4, 32, 33, 55, 192, 154, 97, 38, 149, 45, 41, 232, 92, 250, 21, 17, 47, 203, 39, 85, 59, 163, 254, 37, 104, 204, 155, 181, 227, 60, 184, 62, 213, 90, 223, 169, 30, 68, 81, 70, 120, 216, 56, 28, 228, 29, 64, 43, 57, 16, 71, 24, 83, 136, 78, 86, 87, 88, 231, 186, 156, 164, 74, 89, 95, 106, 98, 108, 99, 123, 141, 122, 103, 190, 109, 137, 127, 146, 0, 249, 91, 67, 94, 100, 168, 112, 207, 116, 119, 150, 121, 65, 248, 124, 125, 126, 23, 128, 158, 61, 201, 132, 19, 175, 110, 73, 8, 138, 139, 142, 96, 222, 196, 22, 145, 115, 52, 197, 44, 66, 31, 152, 199, 253, 46, 111, 194, 187, 14, 167, 159, 7, 79, 225, 51, 202, 209, 239, 3, 170, 171, 234, 129, 224, 244, 176, 177, 130, 6, 180, 13, 174, 54, 53, 185, 178, 217, 188, 189, 229, 191, 133, 63, 157, 20, 49, 18, 198, 153, 140, 212, 76, 48, 193, 77, 206, 107, 208, 131, 210, 151, 205, 117, 11, 215, 240, 42, 101, 219, 220, 221, 247, 58, 102, 84, 36, 118, 2, 218, 230, 143, 161, 241, 1, 235, 236, 237, 135, 75, 226, 147, 15, 50, 34, 245, 246, 113, 144, 165, 242, 251, 252, 162, 238, 255)
1	(25, 198, 134, 79, 114, 184, 152, 11, 108, 23, 217, 173, 231, 200, 8, 201, 72, 69, 121, 124, 183, 212, 172, 147, 211, 123, 233, 27, 80, 20, 252, 88, 45, 209, 214, 192, 17, 60, 38, 149, 32, 41, 199, 216, 240, 31, 236, 244, 162, 39, 171, 116, 106, 254, 37, 164, 92, 42, 232, 99, 138, 219, 0, 93, 90, 223, 175, 47, 255, 195, 181, 120, 241, 157, 28, 228, 62, 52, 18, 57, 178, 97, 56, 83, 136, 78, 221, 87, 70, 188, 186, 73, 59, 143, 67, 113, 86, 74, 207, 197, 155, 158, 122, 206, 190, 109, 115, 203, 146, 84, 225, 63, 61, 34, 248, 174, 50, 179, 182, 131, 16, 36, 82, 100, 242, 95, 150, 9, 128, 250, 159, 105, 125, 19, 91, 110, 226, 235, 243, 1, 142, 96, 222, 196, 193, 126, 168, 64, 227, 44, 66, 10, 229, 51, 141, 85, 111, 4, 176, 14, 185, 224, 101, 53, 140, 48, 160, 169, 180, 102, 253, 245, 35, 204, 21, 46, 166, 177, 49, 144, 187, 13, 145, 29, 137, 167, 210, 33, 26, 189, 71, 191, 133, 40, 24, 98, 130, 213, 104, 153, 249, 148, 76, 54, 89, 77, 103, 107, 208, 215, 139, 151, 205, 117, 65, 119, 129, 202, 7, 5, 220, 30, 12, 58, 3, 22, 6, 118, 2, 218, 239, 247, 161, 170, 246, 81, 154, 237, 135, 75, 43, 94, 230, 112, 163, 15, 55, 132, 234, 165, 194, 251, 156, 127, 238, 68)

Tabulka 3: *pokračování*

Id	Permutace
2	(64, 176, 134, 171, 98, 11, 152, 116, 246, 4, 17, 1, 231, 202, 8, 180, 72, 200, 131, 96, 123, 184, 46, 135, 248, 115, 23, 34, 80, 195, 223, 205, 242, 209, 221, 77, 217, 60, 38, 149, 32, 78, 199, 255, 240, 37, 236, 15, 162, 203, 118, 207, 92, 129, 31, 24, 55, 95, 185, 143, 108, 73, 252, 65, 128, 165, 172, 148, 187, 79, 191, 90, 241, 222, 6, 160, 62, 163, 189, 57, 178, 97, 56, 158, 136, 9, 106, 233, 70, 227, 186, 126, 59, 159, 153, 125, 83, 74, 117, 142, 206, 220, 91, 224, 251, 109, 124, 39, 29, 84, 225, 50, 61, 215, 211, 214, 10, 132, 43, 243, 16, 36, 48, 104, 244, 44, 198, 254, 113, 27, 174, 212, 19, 226, 88, 67, 20, 235, 121, 183, 182, 110, 232, 237, 193, 86, 33, 218, 188, 247, 66, 25, 229, 51, 141, 85, 111, 169, 151, 119, 147, 107, 166, 53, 146, 122, 75, 54, 138, 102, 253, 245, 35, 179, 21, 175, 170, 120, 49, 144, 87, 13, 145, 140, 137, 167, 238, 230, 28, 133, 71, 181, 99, 157, 40, 100, 130, 213, 105, 228, 249, 196, 76, 219, 190, 192, 103, 12, 208, 177, 45, 150, 0, 114, 197, 234, 194, 18, 89, 5, 82, 63, 69, 58, 3, 22, 168, 42, 2, 30, 239, 101, 161, 164, 94, 81, 154, 47, 250, 173, 93, 155, 201, 112, 52, 139, 216, 204, 14, 26, 41, 7, 156, 127, 210, 68)
3	(186, 113, 151, 129, 49, 42, 27, 178, 6, 4, 154, 1, 197, 142, 194, 43, 72, 176, 209, 56, 90, 184, 46, 20, 40, 33, 23, 29, 173, 121, 223, 156, 101, 155, 221, 100, 217, 60, 38, 70, 32, 161, 96, 255, 240, 201, 57, 98, 162, 50, 44, 207, 92, 171, 31, 94, 244, 95, 118, 143, 128, 24, 252, 48, 108, 165, 172, 148, 187, 200, 114, 109, 218, 222, 13, 160, 62, 229, 189, 45, 144, 195, 153, 158, 196, 241, 175, 81, 248, 227, 141, 106, 192, 116, 199, 125, 86, 180, 167, 55, 75, 58, 91, 224, 104, 140, 210, 67, 247, 228, 225, 138, 61, 242, 211, 145, 253, 132, 139, 102, 16, 36, 17, 65, 150, 249, 37, 133, 79, 39, 174, 212, 19, 226, 88, 5, 8, 235, 105, 163, 182, 110, 232, 237, 103, 238, 77, 9, 188, 183, 3, 239, 134, 51, 64, 85, 215, 169, 131, 119, 147, 107, 166, 53, 78, 122, 74, 54, 204, 243, 97, 203, 35, 179, 21, 126, 170, 120, 34, 231, 87, 135, 193, 152, 137, 84, 71, 93, 28, 254, 83, 181, 99, 157, 82, 112, 111, 73, 130, 18, 185, 123, 76, 7, 202, 59, 41, 12, 208, 177, 236, 190, 52, 191, 213, 234, 246, 250, 149, 117, 89, 63, 69, 220, 66, 22, 168, 198, 2, 233, 68, 10, 230, 164, 159, 30, 15, 127, 136, 245, 219, 115, 214, 251, 0, 206, 216, 80, 14, 26, 47, 146, 205, 11, 124, 25)
4	(237, 113, 46, 90, 207, 124, 233, 84, 66, 136, 75, 1, 73, 224, 156, 94, 62, 12, 161, 143, 129, 192, 32, 20, 40, 33, 217, 29, 173, 168, 223, 45, 101, 165, 221, 201, 23, 190, 174, 70, 151, 189, 96, 160, 255, 4, 57, 49, 167, 162, 60, 222, 92, 171, 226, 50, 195, 109, 97, 21, 128, 24, 252, 16, 82, 155, 182, 163, 175, 98, 172, 95, 218, 208, 137, 250, 240, 178, 229, 11, 79, 248, 120, 38, 196, 103, 31, 181, 93, 227, 158, 110, 176, 116, 225, 81, 59, 117, 68, 55, 154, 202, 43, 230, 236, 139, 210, 180, 247, 17, 194, 244, 61, 166, 111, 145, 138, 27, 198, 152, 141, 28, 114, 213, 121, 249, 37, 133, 134, 39, 72, 53, 22, 147, 119, 65, 8, 144, 105, 87, 215, 106, 232, 186, 42, 102, 78, 9, 228, 204, 91, 184, 231, 51, 64, 164, 245, 169, 131, 197, 187, 107, 74, 183, 77, 15, 100, 253, 6, 214, 118, 199, 35, 54, 115, 126, 170, 153, 251, 13, 25, 150, 212, 220, 56, 19, 71, 48, 179, 241, 44, 89, 122, 130, 63, 112, 69, 88, 83, 18, 185, 86, 125, 7, 58, 123, 246, 67, 30, 177, 104, 157, 52, 211, 239, 140, 146, 193, 149, 235, 135, 254, 191, 148, 142, 209, 242, 203, 200, 108, 5, 10, 234, 85, 159, 76, 99, 127, 2, 243, 219, 132, 188, 34, 0, 206, 216, 80, 14, 26, 47, 41, 205, 3, 238, 36)

Tabulka 3: *pokračování*

Id	Permutace
5	(237, 139, 148, 93, 227, 198, 127, 207, 134, 160, 29, 147, 88, 56, 222, 178, 247, 12, 21, 143, 116, 192, 165, 245, 40, 114, 25, 51, 173, 191, 131, 176, 71, 201, 221, 168, 65, 220, 249, 97, 228, 251, 67, 141, 68, 44, 32, 49, 8, 117, 85, 250, 39, 106, 243, 30, 11, 73, 115, 162, 128, 231, 118, 16, 82, 186, 24, 64, 175, 10, 86, 9, 188, 150, 121, 46, 104, 238, 189, 4, 224, 187, 120, 38, 230, 255, 31, 79, 92, 239, 158, 110, 60, 246, 37, 81, 193, 213, 229, 18, 13, 100, 157, 129, 235, 2, 177, 136, 50, 22, 112, 113, 72, 166, 252, 145, 54, 52, 155, 7, 208, 149, 76, 233, 214, 27, 225, 133, 130, 164, 223, 146, 41, 196, 219, 83, 62, 103, 254, 87, 36, 17, 47, 169, 42, 232, 241, 217, 203, 204, 78, 1, 182, 210, 45, 101, 28, 89, 55, 124, 77, 107, 0, 183, 215, 15, 195, 153, 5, 180, 111, 199, 35, 138, 66, 126, 170, 212, 172, 119, 200, 23, 253, 190, 61, 19, 234, 216, 137, 132, 226, 43, 154, 90, 63, 179, 69, 59, 6, 202, 185, 94, 218, 142, 58, 144, 95, 96, 74, 244, 151, 197, 123, 211, 167, 140, 53, 48, 70, 236, 135, 171, 75, 102, 84, 209, 242, 108, 122, 125, 57, 98, 174, 194, 156, 33, 109, 20, 159, 161, 181, 240, 248, 34, 80, 206, 163, 184, 14, 26, 152, 99, 205, 3, 105, 91)
6	(226, 198, 152, 14, 242, 158, 213, 253, 227, 34, 97, 10, 190, 45, 115, 81, 231, 66, 214, 143, 116, 180, 90, 245, 70, 121, 20, 51, 239, 22, 113, 4, 33, 35, 221, 53, 196, 220, 120, 55, 82, 99, 191, 177, 144, 44, 162, 182, 156, 174, 128, 250, 104, 106, 243, 222, 11, 85, 1, 95, 110, 25, 141, 17, 126, 186, 24, 131, 175, 249, 114, 189, 188, 36, 56, 46, 223, 130, 195, 63, 197, 148, 179, 173, 228, 255, 83, 146, 2, 3, 157, 225, 60, 201, 37, 30, 78, 48, 57, 125, 163, 166, 254, 109, 193, 181, 217, 107, 142, 251, 112, 184, 72, 73, 236, 145, 96, 59, 155, 58, 208, 13, 68, 233, 168, 176, 67, 23, 40, 74, 28, 210, 41, 165, 71, 100, 62, 103, 87, 9, 89, 16, 92, 32, 42, 43, 94, 194, 7, 65, 29, 202, 132, 136, 187, 101, 218, 49, 21, 124, 77, 164, 200, 54, 98, 84, 93, 50, 5, 8, 52, 199, 216, 27, 6, 185, 170, 212, 31, 219, 150, 133, 244, 88, 153, 19, 241, 248, 0, 172, 232, 139, 154, 18, 192, 167, 234, 111, 252, 224, 230, 178, 206, 61, 160, 69, 119, 203, 215, 149, 151, 76, 240, 207, 137, 140, 135, 86, 123, 211, 209, 171, 75, 102, 15, 122, 247, 108, 183, 26, 237, 12, 204, 134, 127, 64, 129, 147, 159, 161, 47, 38, 79, 169, 117, 118, 138, 235, 238, 39, 246, 229, 205, 80, 105, 91)
7	(72, 224, 173, 134, 208, 143, 235, 236, 102, 222, 97, 137, 111, 212, 16, 31, 86, 159, 214, 221, 116, 180, 90, 191, 52, 49, 168, 121, 239, 21, 205, 4, 47, 218, 149, 43, 89, 220, 106, 215, 82, 78, 187, 177, 144, 237, 150, 249, 22, 174, 68, 219, 125, 62, 10, 242, 140, 120, 15, 95, 133, 203, 141, 17, 126, 250, 55, 255, 175, 105, 129, 101, 188, 28, 69, 46, 201, 13, 128, 27, 93, 148, 179, 108, 228, 247, 36, 213, 234, 3, 196, 152, 186, 182, 37, 80, 99, 48, 35, 135, 243, 166, 254, 20, 103, 181, 198, 107, 240, 185, 112, 176, 85, 190, 165, 145, 96, 24, 251, 192, 226, 130, 94, 38, 19, 151, 155, 23, 225, 138, 66, 210, 41, 253, 245, 70, 44, 29, 7, 83, 157, 2, 164, 32, 8, 53, 56, 131, 26, 197, 91, 227, 132, 98, 71, 189, 170, 51, 142, 124, 162, 146, 200, 54, 114, 84, 58, 217, 59, 156, 5, 136, 207, 60, 6, 63, 57, 223, 244, 25, 39, 115, 45, 73, 153, 100, 241, 248, 0, 172, 232, 139, 154, 119, 65, 167, 169, 42, 252, 194, 230, 178, 206, 61, 160, 195, 18, 88, 158, 184, 163, 76, 11, 117, 92, 34, 123, 231, 104, 211, 209, 171, 75, 110, 1, 113, 193, 109, 40, 216, 9, 77, 204, 14, 127, 64, 199, 87, 67, 161, 33, 233, 79, 147, 30, 118, 74, 183, 238, 12, 246, 229, 122, 50, 81, 202)

Tabulka 3: *pokračování*

Id	Permutace
8	(72, 254, 192, 32, 208, 216, 95, 236, 102, 187, 97, 21, 48, 212, 193, 168, 93, 159, 214, 234, 143, 144, 19, 184, 229, 131, 227, 121, 165, 137, 83, 69, 30, 50, 171, 43, 244, 204, 106, 215, 82, 78, 40, 177, 213, 120, 150, 221, 122, 224, 68, 34, 125, 62, 200, 20, 49, 237, 243, 235, 88, 71, 111, 17, 126, 230, 202, 255, 175, 105, 26, 196, 188, 56, 28, 182, 25, 41, 114, 27, 190, 148, 79, 158, 157, 247, 203, 1, 123, 47, 127, 152, 186, 89, 86, 80, 99, 195, 35, 223, 198, 189, 2, 180, 118, 181, 211, 233, 240, 185, 197, 245, 85, 87, 225, 145, 7, 24, 251, 226, 206, 130, 249, 135, 140, 36, 91, 199, 18, 138, 66, 14, 13, 248, 176, 55, 101, 29, 96, 220, 222, 10, 164, 252, 8, 53, 65, 44, 52, 250, 155, 151, 90, 98, 183, 112, 166, 51, 142, 210, 162, 163, 174, 173, 12, 147, 58, 217, 113, 156, 5, 201, 207, 124, 67, 179, 57, 38, 242, 37, 3, 92, 228, 117, 253, 100, 241, 16, 0, 129, 232, 139, 191, 119, 4, 167, 169, 42, 141, 194, 170, 149, 239, 60, 134, 115, 64, 133, 108, 136, 15, 54, 11, 73, 9, 161, 94, 231, 39, 63, 31, 178, 109, 74, 61, 59, 6, 128, 103, 205, 146, 76, 75, 46, 160, 104, 23, 154, 209, 219, 33, 107, 45, 84, 218, 77, 110, 70, 238, 153, 246, 172, 132, 116, 81, 22)
9	(7, 254, 170, 0, 208, 56, 248, 155, 102, 149, 234, 24, 48, 90, 32, 203, 93, 9, 1, 219, 226, 144, 19, 212, 229, 75, 227, 195, 165, 205, 217, 194, 251, 142, 201, 43, 99, 84, 145, 215, 82, 78, 120, 177, 173, 40, 150, 221, 122, 30, 103, 5, 125, 228, 31, 20, 253, 4, 166, 156, 88, 12, 111, 80, 236, 230, 101, 246, 175, 113, 135, 172, 188, 51, 106, 157, 130, 41, 26, 83, 190, 148, 33, 62, 35, 247, 85, 211, 49, 224, 127, 152, 255, 139, 86, 36, 232, 121, 91, 214, 231, 242, 2, 180, 13, 181, 108, 233, 25, 185, 44, 235, 3, 87, 225, 198, 216, 17, 47, 200, 210, 132, 60, 186, 126, 174, 105, 199, 18, 184, 114, 193, 57, 243, 182, 223, 202, 140, 96, 14, 52, 10, 11, 252, 92, 189, 65, 154, 222, 250, 68, 54, 131, 98, 183, 187, 23, 28, 50, 70, 178, 163, 240, 213, 71, 147, 58, 27, 21, 67, 204, 116, 207, 124, 245, 220, 109, 38, 95, 37, 168, 8, 112, 117, 16, 34, 241, 79, 45, 129, 244, 89, 191, 119, 107, 176, 169, 42, 151, 69, 192, 123, 55, 66, 171, 162, 64, 133, 72, 136, 15, 141, 22, 73, 159, 161, 94, 134, 39, 63, 143, 115, 158, 74, 61, 59, 6, 128, 29, 137, 146, 76, 100, 46, 160, 104, 53, 239, 249, 196, 118, 237, 197, 138, 218, 77, 110, 206, 179, 153, 167, 238, 209, 97, 81, 164)
10	(133, 114, 115, 215, 221, 129, 87, 233, 110, 25, 234, 152, 158, 165, 216, 139, 138, 190, 200, 248, 226, 250, 19, 64, 71, 168, 65, 48, 70, 20, 142, 194, 59, 85, 58, 34, 207, 199, 229, 181, 134, 220, 219, 177, 52, 202, 150, 112, 171, 224, 203, 17, 170, 68, 29, 7, 39, 13, 148, 109, 137, 246, 14, 225, 236, 231, 228, 28, 162, 154, 157, 117, 86, 1, 26, 197, 130, 41, 106, 183, 223, 84, 12, 160, 143, 108, 136, 211, 99, 96, 32, 166, 128, 4, 217, 36, 120, 91, 196, 227, 179, 77, 31, 205, 172, 56, 247, 43, 149, 169, 253, 103, 3, 113, 61, 208, 50, 174, 185, 15, 49, 6, 60, 9, 0, 182, 145, 192, 18, 101, 214, 193, 57, 42, 66, 24, 135, 140, 79, 254, 131, 155, 126, 121, 92, 187, 188, 213, 222, 10, 54, 123, 206, 27, 83, 249, 8, 107, 122, 102, 178, 141, 81, 78, 238, 237, 67, 74, 90, 159, 167, 241, 127, 124, 93, 125, 156, 38, 51, 147, 37, 21, 75, 46, 251, 40, 62, 189, 239, 252, 244, 73, 191, 119, 240, 176, 209, 2, 23, 76, 88, 232, 198, 255, 72, 16, 35, 243, 80, 82, 163, 95, 151, 94, 210, 204, 173, 235, 33, 63, 44, 98, 245, 111, 47, 144, 132, 230, 212, 30, 175, 69, 100, 201, 53, 161, 164, 45, 55, 146, 118, 105, 116, 184, 218, 104, 97, 22, 195, 186, 153, 89, 11, 5, 242, 180)

Tabulka 3: *pokračování*

Id	Permutace
11	(27, 84, 13, 29, 219, 226, 65, 15, 203, 152, 170, 230, 158, 90, 181, 63, 76, 248, 118, 73, 196, 216, 77, 38, 8, 231, 136, 34, 68, 54, 58, 194, 106, 20, 156, 48, 57, 18, 229, 113, 69, 139, 9, 177, 146, 202, 163, 143, 171, 101, 251, 23, 147, 108, 4, 233, 71, 185, 150, 102, 214, 186, 14, 80, 236, 189, 133, 83, 55, 201, 224, 141, 24, 1, 26, 110, 123, 246, 157, 207, 19, 60, 222, 160, 45, 164, 244, 36, 250, 228, 190, 166, 174, 255, 217, 191, 74, 91, 240, 44, 179, 97, 142, 16, 197, 182, 195, 88, 154, 169, 41, 178, 51, 39, 87, 89, 135, 43, 105, 122, 206, 112, 99, 111, 85, 241, 145, 114, 66, 215, 199, 115, 172, 56, 242, 10, 61, 78, 237, 95, 131, 119, 3, 121, 22, 129, 81, 223, 159, 86, 239, 192, 100, 167, 253, 249, 32, 107, 93, 109, 148, 162, 234, 188, 49, 79, 238, 138, 165, 183, 144, 62, 127, 124, 2, 96, 213, 140, 193, 0, 64, 175, 180, 198, 6, 252, 52, 75, 200, 218, 98, 134, 151, 132, 155, 67, 209, 7, 17, 247, 46, 232, 53, 37, 130, 211, 35, 221, 225, 187, 40, 227, 33, 70, 31, 137, 173, 205, 12, 220, 50, 116, 245, 128, 47, 59, 72, 25, 212, 21, 254, 28, 149, 243, 161, 120, 208, 11, 126, 235, 125, 117, 184, 30, 94, 104, 42, 176, 210, 103, 153, 204, 82, 5, 92, 168)
12	(27, 84, 13, 29, 219, 226, 28, 15, 203, 152, 170, 230, 158, 90, 181, 63, 76, 248, 118, 73, 196, 216, 77, 38, 8, 231, 136, 34, 68, 54, 253, 194, 106, 20, 156, 48, 57, 70, 228, 113, 69, 44, 9, 87, 146, 202, 163, 143, 171, 101, 251, 23, 157, 108, 4, 233, 71, 185, 150, 102, 214, 186, 14, 209, 236, 189, 133, 83, 55, 201, 224, 172, 24, 1, 26, 193, 123, 246, 147, 207, 19, 60, 211, 160, 126, 179, 244, 161, 250, 229, 190, 166, 174, 255, 217, 191, 74, 91, 240, 139, 164, 97, 142, 16, 197, 232, 195, 88, 154, 169, 41, 178, 51, 39, 177, 89, 132, 43, 105, 122, 206, 112, 99, 111, 85, 241, 145, 215, 66, 114, 199, 198, 144, 56, 242, 10, 61, 78, 237, 95, 131, 119, 3, 121, 116, 80, 81, 223, 159, 86, 239, 192, 100, 167, 58, 249, 32, 107, 93, 109, 148, 162, 234, 188, 128, 96, 238, 138, 127, 183, 141, 62, 129, 124, 2, 79, 213, 140, 137, 0, 64, 175, 180, 115, 6, 49, 52, 75, 218, 200, 98, 134, 151, 135, 155, 210, 165, 7, 17, 247, 46, 182, 53, 37, 130, 222, 35, 221, 225, 187, 40, 227, 33, 18, 31, 110, 173, 205, 12, 220, 50, 22, 245, 252, 47, 59, 72, 25, 212, 21, 254, 65, 149, 243, 36, 120, 208, 11, 45, 235, 125, 117, 184, 30, 94, 104, 42, 176, 67, 103, 153, 204, 82, 5, 92, 168)

Tabulka 3: *pokračování*

Id	Permutace
13	(122, 174, 140, 161, 246, 127, 199, 44, 40, 252, 57, 215, 3, 19, 162, 69, 76, 158, 146, 45, 159, 177, 77, 38, 78, 231, 219, 34, 29, 103, 5, 82, 106, 20, 156, 73, 68, 70, 251, 202, 149, 15, 9, 247, 118, 60, 163, 21, 13, 52, 130, 218, 157, 108, 7, 32, 72, 1, 182, 64, 214, 186, 14, 209, 55, 224, 93, 168, 236, 152, 245, 133, 160, 129, 50, 116, 123, 230, 147, 197, 90, 107, 138, 86, 71, 179, 244, 59, 242, 100, 191, 235, 194, 213, 61, 99, 74, 237, 22, 30, 164, 96, 4, 238, 207, 31, 195, 234, 131, 113, 185, 200, 203, 16, 167, 212, 66, 148, 105, 183, 206, 83, 109, 49, 12, 241, 121, 89, 132, 67, 28, 97, 92, 56, 250, 10, 255, 139, 220, 110, 154, 119, 201, 0, 112, 135, 81, 217, 87, 150, 84, 181, 41, 210, 98, 249, 227, 198, 126, 248, 190, 173, 223, 188, 155, 39, 85, 62, 48, 178, 211, 18, 136, 124, 2, 79, 8, 24, 128, 46, 125, 175, 180, 33, 6, 205, 253, 94, 23, 27, 65, 225, 232, 36, 137, 169, 240, 142, 17, 47, 102, 187, 53, 229, 114, 222, 63, 172, 134, 43, 35, 145, 115, 58, 171, 165, 192, 153, 141, 91, 26, 196, 88, 25, 189, 208, 184, 54, 143, 37, 204, 151, 51, 243, 176, 120, 193, 11, 144, 166, 216, 117, 80, 101, 75, 254, 42, 95, 233, 111, 239, 221, 228, 170, 104, 226)
14	(191, 18, 140, 155, 151, 91, 175, 125, 31, 115, 158, 172, 3, 111, 208, 254, 210, 68, 146, 203, 64, 55, 234, 76, 63, 103, 174, 207, 119, 239, 213, 40, 106, 169, 156, 230, 50, 128, 197, 79, 218, 122, 85, 247, 118, 229, 163, 56, 69, 78, 171, 145, 98, 232, 7, 94, 45, 49, 0, 21, 11, 152, 14, 209, 87, 112, 93, 36, 26, 138, 222, 217, 129, 134, 105, 88, 62, 65, 201, 10, 90, 231, 205, 2, 246, 23, 44, 13, 242, 12, 182, 248, 193, 61, 83, 236, 99, 81, 27, 221, 9, 235, 4, 189, 139, 255, 82, 16, 39, 184, 162, 226, 164, 47, 224, 17, 37, 148, 38, 179, 206, 228, 46, 166, 77, 227, 43, 194, 25, 67, 28, 97, 33, 92, 8, 147, 35, 192, 220, 167, 250, 121, 48, 173, 188, 58, 126, 159, 110, 244, 84, 57, 102, 22, 216, 249, 199, 42, 202, 51, 195, 241, 223, 1, 165, 176, 41, 74, 66, 149, 211, 237, 34, 124, 60, 89, 131, 24, 245, 178, 80, 214, 136, 161, 108, 186, 181, 20, 71, 238, 72, 6, 19, 127, 150, 132, 219, 109, 170, 53, 154, 187, 190, 104, 114, 70, 52, 225, 153, 29, 215, 252, 137, 185, 233, 183, 196, 253, 243, 160, 96, 157, 107, 141, 212, 251, 113, 54, 143, 73, 240, 116, 180, 135, 177, 120, 86, 30, 144, 59, 5, 200, 142, 101, 75, 32, 198, 95, 130, 123, 100, 133, 168, 15, 117, 204)
15	(254, 18, 33, 155, 151, 200, 96, 125, 31, 244, 158, 242, 3, 111, 208, 191, 240, 68, 146, 203, 64, 55, 234, 73, 235, 103, 137, 207, 119, 239, 213, 70, 241, 169, 106, 230, 50, 128, 197, 79, 218, 122, 85, 247, 118, 229, 196, 56, 181, 38, 171, 145, 98, 34, 7, 94, 45, 149, 0, 21, 74, 152, 14, 184, 87, 112, 121, 36, 99, 47, 222, 217, 129, 134, 105, 138, 62, 65, 102, 248, 90, 231, 205, 108, 246, 209, 44, 13, 172, 5, 182, 81, 193, 57, 83, 236, 12, 210, 27, 221, 9, 63, 11, 189, 139, 255, 82, 16, 71, 249, 162, 226, 164, 88, 228, 17, 37, 148, 120, 179, 206, 201, 46, 166, 77, 227, 214, 135, 25, 67, 28, 97, 140, 92, 8, 147, 35, 192, 174, 167, 250, 173, 48, 93, 232, 58, 126, 159, 175, 115, 84, 61, 19, 22, 216, 224, 199, 42, 202, 51, 195, 156, 223, 1, 165, 219, 185, 4, 66, 49, 59, 220, 188, 132, 60, 89, 131, 24, 245, 178, 80, 43, 39, 161, 2, 186, 69, 160, 136, 238, 72, 6, 23, 113, 150, 124, 176, 109, 170, 53, 154, 187, 190, 104, 114, 40, 52, 225, 153, 29, 215, 252, 237, 41, 233, 183, 163, 253, 243, 20, 110, 157, 107, 141, 212, 251, 127, 54, 143, 76, 10, 116, 180, 194, 177, 78, 86, 30, 26, 91, 144, 142, 211, 101, 75, 32, 198, 95, 130, 123, 100, 133, 168, 15, 117, 204)

Tabulka 3: *pokračování*

Id	Permutace
16	(254, 191, 85, 73, 91, 200, 87, 45, 72, 33, 158, 48, 217, 115, 41, 110, 16, 101, 231, 96, 141, 213, 223, 121, 232, 195, 211, 92, 67, 198, 76, 36, 118, 86, 18, 134, 52, 128, 11, 8, 155, 19, 247, 81, 241, 206, 215, 114, 65, 124, 171, 145, 56, 34, 159, 62, 44, 162, 246, 117, 23, 89, 194, 184, 248, 218, 192, 142, 230, 245, 202, 135, 199, 79, 105, 138, 157, 143, 102, 168, 90, 164, 205, 22, 178, 209, 187, 13, 126, 98, 153, 104, 51, 169, 83, 221, 12, 210, 154, 137, 222, 131, 70, 189, 139, 255, 166, 220, 71, 239, 116, 226, 225, 238, 1, 35, 212, 129, 216, 179, 25, 201, 229, 68, 77, 249, 64, 234, 29, 250, 172, 95, 119, 228, 224, 147, 94, 244, 170, 186, 43, 242, 173, 93, 10, 151, 7, 69, 49, 177, 78, 61, 57, 46, 17, 122, 136, 42, 0, 97, 103, 149, 24, 14, 165, 58, 160, 207, 66, 63, 111, 144, 188, 132, 55, 167, 120, 38, 74, 146, 214, 26, 39, 40, 2, 30, 125, 204, 108, 251, 82, 6, 240, 109, 203, 163, 176, 88, 174, 53, 140, 37, 190, 236, 99, 197, 15, 9, 5, 54, 196, 252, 237, 208, 233, 183, 156, 253, 243, 20, 235, 185, 107, 59, 84, 47, 127, 60, 161, 27, 175, 133, 180, 112, 219, 113, 181, 227, 106, 3, 50, 152, 28, 31, 75, 32, 4, 193, 130, 123, 100, 148, 80, 150, 21, 182)
17	(202, 191, 85, 73, 6, 208, 87, 12, 72, 189, 158, 165, 59, 115, 135, 124, 129, 1, 116, 226, 221, 213, 60, 199, 105, 152, 196, 92, 112, 198, 214, 119, 134, 125, 100, 3, 52, 27, 11, 95, 80, 19, 235, 84, 241, 67, 215, 254, 65, 103, 190, 90, 77, 7, 185, 62, 99, 162, 246, 86, 23, 32, 4, 34, 248, 203, 178, 13, 230, 245, 44, 41, 242, 79, 64, 58, 157, 136, 102, 167, 76, 142, 20, 113, 192, 66, 187, 164, 126, 98, 14, 109, 170, 159, 83, 146, 238, 249, 154, 35, 222, 57, 243, 33, 183, 210, 74, 220, 71, 131, 175, 252, 225, 128, 169, 111, 255, 56, 216, 179, 25, 206, 207, 101, 18, 232, 171, 234, 29, 150, 16, 200, 218, 114, 209, 147, 212, 121, 46, 186, 120, 30, 117, 93, 91, 130, 61, 227, 49, 177, 78, 36, 193, 81, 237, 122, 8, 42, 0, 45, 181, 149, 217, 188, 195, 138, 140, 219, 224, 26, 40, 17, 137, 10, 55, 70, 21, 75, 166, 250, 145, 231, 39, 153, 2, 54, 143, 204, 108, 148, 82, 151, 211, 173, 223, 69, 176, 88, 174, 96, 229, 156, 163, 236, 144, 197, 37, 9, 5, 184, 240, 53, 228, 104, 233, 89, 15, 253, 168, 118, 247, 205, 107, 51, 244, 97, 127, 172, 161, 47, 24, 133, 180, 201, 194, 22, 139, 94, 106, 63, 50, 48, 28, 31, 132, 38, 160, 110, 239, 123, 68, 251, 155, 141, 43, 182)
18	(202, 81, 85, 249, 6, 70, 87, 18, 150, 189, 158, 165, 188, 127, 108, 124, 222, 1, 116, 226, 214, 119, 193, 199, 105, 152, 196, 92, 63, 198, 213, 221, 134, 125, 143, 4, 114, 27, 154, 136, 80, 8, 49, 84, 121, 67, 215, 254, 65, 234, 190, 153, 77, 237, 185, 62, 251, 162, 179, 86, 23, 32, 3, 109, 224, 123, 178, 13, 230, 245, 44, 41, 59, 207, 64, 58, 157, 53, 102, 167, 76, 142, 20, 113, 192, 181, 187, 95, 126, 98, 14, 0, 170, 201, 248, 146, 238, 73, 11, 155, 253, 57, 71, 33, 183, 210, 74, 220, 169, 204, 55, 131, 225, 242, 104, 12, 255, 56, 130, 246, 147, 206, 129, 182, 26, 54, 5, 103, 29, 72, 128, 200, 218, 52, 209, 25, 212, 83, 168, 186, 120, 159, 117, 93, 91, 216, 61, 66, 235, 9, 78, 36, 60, 191, 7, 122, 19, 239, 34, 45, 31, 149, 217, 227, 195, 138, 141, 219, 171, 111, 40, 17, 164, 10, 175, 247, 21, 75, 166, 250, 145, 16, 148, 15, 243, 232, 22, 252, 135, 39, 82, 151, 211, 173, 223, 69, 110, 160, 174, 30, 229, 156, 163, 236, 144, 197, 37, 140, 35, 184, 240, 96, 228, 99, 233, 89, 90, 79, 46, 118, 208, 205, 38, 51, 244, 97, 115, 172, 161, 177, 24, 133, 180, 137, 194, 100, 139, 94, 106, 112, 50, 48, 28, 231, 132, 107, 88, 176, 42, 203, 68, 2, 241, 47, 43, 101)

Tabulka 3: *pokračování*

Id	Permutace
19	(159, 81, 85, 249, 57, 90, 87, 238, 150, 189, 158, 228, 188, 127, 108, 124, 144, 1, 116, 177, 164, 23, 193, 199, 74, 152, 149, 236, 63, 198, 207, 101, 134, 125, 221, 4, 114, 27, 104, 10, 80, 8, 49, 84, 200, 136, 215, 254, 77, 234, 190, 229, 65, 176, 185, 107, 251, 162, 22, 86, 119, 250, 3, 154, 224, 123, 178, 13, 161, 231, 44, 41, 59, 169, 64, 58, 157, 96, 21, 167, 76, 142, 20, 113, 192, 137, 187, 235, 126, 62, 14, 0, 170, 201, 248, 146, 7, 122, 11, 155, 253, 60, 186, 33, 183, 210, 115, 182, 211, 204, 55, 131, 225, 139, 109, 12, 255, 56, 130, 246, 15, 206, 174, 79, 9, 54, 151, 141, 29, 72, 128, 94, 218, 52, 209, 25, 212, 83, 168, 71, 120, 202, 117, 93, 51, 216, 6, 66, 172, 140, 78, 214, 46, 191, 18, 73, 61, 239, 24, 45, 31, 242, 230, 227, 195, 138, 103, 219, 171, 111, 40, 89, 36, 160, 175, 247, 102, 75, 166, 180, 145, 16, 220, 147, 35, 232, 179, 252, 135, 38, 82, 121, 50, 173, 223, 69, 92, 67, 129, 30, 153, 5, 163, 110, 222, 197, 37, 196, 243, 184, 240, 53, 165, 99, 233, 17, 70, 43, 19, 118, 208, 205, 39, 91, 244, 97, 105, 95, 217, 226, 34, 133, 32, 181, 194, 100, 26, 156, 106, 112, 213, 48, 28, 245, 132, 148, 88, 237, 42, 203, 68, 2, 241, 47, 98, 143)

C Seznam testovaných kvazigrup, řazeno podle identifikačního čísla kvazigupy

Tento seznam je velmi rozměrný(cca 200 stran), je tudíž v obsahu přiloženého DVD v souboru *TestovaneKvazigrupyID.pdf*.

D Seznam testovaných kvazigrup, řazeno podle vlastností

Je to stejný seznam jak v předchozí kapitole, pouze je jinak setříděn. Opět v obsahu DVD v souboru *TestovaneKvazigrupyVlastnosti.pdf*.

E Protokoly s vyhodnocením experimentů

Dále je v DVD obsažen soubor *Protokoly.ps*, kde jsou shrnuty experimentalní výsledky. Pro každou kvazigrupu jsou uvedena všecha získaná data včetně grafů.